SECURITY FOR BUILDING OCCUPANTS AND ASSETS

1 Purpose

The purpose of this lesson set is to provide students with three levels of involvement with the subject content: to explore the multiple issues of federal building security, to introduce concepts of five levels of federal building security; to apply the fifty-two accepted security standard practices for federal buildings. Each is to be engaged in one of three sequenced class sessions.

2 Duration of Lesson

50 Minutes for each session (one per day)

3 Objectives

- Frame an awareness of types of attacks--threat assessment
- Develop an understanding of building vulnerabilities assessment
- Demonstrate an ability to conduct a risk analysis

Depending on the building type, acceptable levels of risk, and decisions made based on recommendations from a comprehensive threat assessment, vulnerability assessment, and risk analysis, appropriate countermeasures should be implemented to protect people, assets, and mission. Types of attack and threats to consider include:

- Unauthorized entry (forced and covert)
- Insider threats
- Explosive threats: Stationary and moving vehicle-delivered, mail bombs, package bombs
- Ballistic threats: Small arms, high-powered rifles, drive-by shootings, etc.
- Weapons of mass destruction (chemical, biological, and radiological)
- Cyber and information security threats

4 Standards & Benchmarks ..... SOCIAL STUDIES

United States Government

Students will identify and define ideas at the core of government and politics in the United States, interpret Founding-Era documents and events associated with the core ideas, and explain how commitment to these foundational ideas constitutes a common American civic identity. They will also analyze issues about the meaning and application of these core ideas to government, politics and civic life, and demonstrate how citizens use these foundational ideas in civic and political life. **USG.2**

Define and provide historical and contemporary examples of fundamental principles and values of American political and civic life, including liberty, security, the common good, justice, equality, law and order, rights of individuals, and social diversity. (Core Standard) **USG.2.5**

Geography And History Of The World

Students will examine the physical and human geographic factors associated with examples of how humans interact with the environment, such as deforestation, natural hazards and the spread of diseases, and the regional and global consequences of these interactions. **GHW.9**

Use maps to identify regions in the world where particular natural disasters occur frequently. Analyze how the physical and human environments in these regions have been modified over time in response to environmental threats. Give examples of how international efforts bring aid to these regions and assess the success of these efforts. **GHW.9.1**

Example: Japan (earthquakes): building reinforced skyscrapers, training for emergency in a disciplined society; United States (hurricanes): the response in Florida and Louisiana, government aid, flood-prone areas in urban environment; Indian Ocean (earthquakes, tsunamis): lack of warning systems in the third world countries, worldwide relief efforts, foreign aid; Colombia (volcanoes): mud-flows, government response in remote areas of the world; Pakistan (earthquakes): remote areas, lack of building codes, terrorist activity; and China (floods): deadly floods on the Hwang Ho River.

5 Vocabulary

The following terms will be used in this lesson.

Unauthorized Entry (Forced and Covert): Protecting the facility and assets from unauthorized persons is an important part of any security system. Some items to consider include:

- Compound or facility access control

  o Control perimeter: Fences, bollards, anti-ram barriers
  o Traffic control, remote controlled gates, anti-ram hydraulic drop arms, and hydraulic barriers, parking
  o Forced-Entry-Ballistic Resistant (FE-BR) doors and windows

- Perimeter intrusion detection systems

  o Clear zone
  o Video and CCTV
  o Alarms
  o Detection devices (motion, acoustic, infrared)

- Personnel identification systems

  o Access control, fingerprints, biometrics, ID cards

- Protection of information and data

  o Acoustic shielding
  o Shielding of electronic security devices from hostile electronic environment
  o Secure access to equipment, networks, and hardware, e.g. satellites and telephone systems

Insider Threats: One of the most serious threats may come from persons who have authorized access to a facility. These may include disgruntled employees or persons who have gained access through normal means (e.g., contractors, support personnel, etc). To mitigate this threat some items to consider include:

- Implement personnel reliability programs and background checks

- Limit and control access to sensitive areas of the facility

Explosive Threats: Stationary and Moving Vehicle-Delivered, Mail Bombs, Package Bombs:

Explosive threats tend to be the criminal and terrorist weapon of choice. Devices may include large amounts of explosives that require delivery by a vehicle. However, smaller amounts may be introduced into a facility through mail, packages, or simply hand carried in an unsecured area. Normally the best defense is to provide defended distance between the threat location and the asset to be protected. This is typically called standoff distance. If standoff is not available or is insufficient to reduce the blast forces reaching the protected asset, structural hardening may be required. If introduced early in the design process, this may be done in an efficient and cost-effective manner. If introduced late in a design, or if retrofitting an existing facility, such a measure may prove to be economically difficult to justify. Some items to consider include:

- The design team should include qualified security and blast consulting professionals from the concept stage forward.
- Provide defended standoff with rated or certified devices such as fencing, bollards, planters, landscaping, or other measures that will stop persons, if required, and vehicle delivered threats.
- Consider structural hardening and hazard mitigation designs such as ductile framing that is capable of withstanding abnormal loads and preventing progressive collapse, protective glazing, strengthening of walls, roofs, and other facility components.
- Design the facility with redundant egress and other critical infrastructure to facilitate emergency evacuation and control during an event.

Ballistic Threats: These threats may range from random drive-by shootings to high-powered rifle attacks directed at specific targets within the facility. It is important to quantify the potential risk and to establish the appropriate level of protection. The most common ballistic protection rating systems include: Underwriters Laboratories (UL), National Institute of Justice (NIJ), H.P. White Laboratory, and ASTM International. Materials are rated based on their ability to stop specific ammunition (e.g., projectile size and velocity). Some items to consider include:

- Visual shielding, such as opaque windows or screening devices
- Ballistic resistant rated materials and products
- Locating critical assets away from direct lines of sight

Weapons of Mass Destruction: Chemical, Biological, and Radiological (CBR)

Commonly referred to as WMD, these threats generally have a low probability of occurrence but the consequences of an attack may be extremely high. While fully protecting a facility against such threats may not be feasible with the exception of very special facilities, there are several common sense and low cost measures that can improve resistance and reduce the risk from the WMD threat. Some items to consider include:

- Protect pathways into the building

  o Control access to air inlets and water systems
  o Provide detection and filtration systems for HVAC systems
  o Provide for emergency HVAC shutoff and control
  o Segregate portions of building spaces (i.e., provide separate HVAC for the lobby, loading docks, and the core of the building)
  o Consider providing positive pressurization to keep contaminates outside of the facility

- Provide an emergency notification system to facilitate orderly response and evacuation.

Cyber and Information Security Threats: In today's world, business continuity and mission function rely heavily on the transmission, storage, and access to a wide range of electronic data and communication systems. It is common to consider the protection of these systems from cyber threats, such as viruses and malware. Protecting these systems from physical attack is just as critical for most users ranging from individuals, businesses, and government agencies. Some items to consider include:

- Understand and identify the information assets that you are trying to protect. These may include personal information, business information such as proprietary designs or processes, national security information, or simply the ability of your organization to communicate via email and other LAN/WAN functions.

- Protect the physical infrastructure that supports information systems. For example, if your computer system is electronically secure but is vulnerable to physical destruction you may not have achieved an adequate level of protection.

- Provide software and hardware devices to detect, monitor, and prevent unauthorized access to or the destruction of sensitive information.

Development and Training on Occupant Emergency Plans:

Occupant Emergency Plans should be developed for building Operations staff and occupants to be able to respond to all forms of credible attacks and threats. Clearly defined lines of communication, responsibilities, and operational procedures are all important parts of Emergency Plans. Emergency Plans are an essential element of protecting life and property from attacks and threats by preparing for and carrying out activities to prevent or minimize personal injury and physical damage. This will be accomplished by pre-emergency planning; establishing specific functions for Operational staff and occupants; training Organization personnel in appropriate functions; instructing occupants of appropriate responses to emergency situations and evacuation procedures; and conducting actual drills.

6 Materials

Computer in classroom with internet connection; Audio and Video Output Devices for the Computer; In-class Worksheets and Handouts

7 Additional Resources

Building / Space Types
Applicable to most building types and space types.

Design Objectives
Aesthetics—Engage the Integrated Design Process, Cost-Effective, Functional / Operational, Historic Preservation, Productive, Secure / Safe, Sustainable

Project Management
Project Planning and Development, Building Commissioning

Tools
LEED®-DoD Antiterrorism Standards Tool

Federal Agencies
All-Hazard Mitigation Program on Anti-terrorism—Federal Emergency Management Agency (FEMA)

Office of Federal Protective Service (FPS)—Security organization that provides Threat and Vulnerability and Risk Assessments and operational security at federal facilities managed by GSA.

Design and Analysis Tools

FSR-Manager—Proprietary software developed by Applied Research Associates, Inc. (ARA) to assist in performing threat/vulnerability assessments and risk analyses

RAMPART™ (Risk Assessment Method—Property Analysis and Ranking Tool)—Developed by Sandia National Laboratories as a screening-level software program to determine the risk to a building by natural hazards, crime, and terrorism

Organizations and Associations

American Society of Industrial Security (ASIS)—A leading non-profit association of security managers, product manufacturers, and consultants offering a variety of publications and programs including Threat and Vulnerability Assessment training

International Association of Professional Security Consultants—An association of security consultants whose members frequently perform Vulnerability Assessments

Publications

Are Your Tenants Safe? by Building Owners and Managers Association. Provides a template and instructions for completing a Threat, Vulnerability and Risk Assessment on commercial and institutional properties. Availability: BOMA

Multi-hazard Identification and Risk Assessment: A Cornerstone of the National Mitigation Strategy by Federal Emergency Management Agency (FEMA). Washington, DC: U.S. Government Printing Office, 1997. Availability: FEMA

8 Procedures & Methods

A. Introduction

A Department of Justice study called "Vulnerability Assessment of Federal Facilities", conducted in response to a Presidential directive and issued one day after the 19 April 1995 Oklahoma City bombing, produced recommended minimum standards for security at federal facilities. It divided federal sites into five security levels ranging from Level 1 (minimum security needs) to Level 5 (maximum). The study listed recommendations for upgrading federal building security, including 52 security standards addressing such items as parking, lighting, physical barriers, and closed circuit television monitoring.

B. Development

Day 1___Students are divided into five groups and each are asked to choose one if the security levels and prepare a presentation on the distinct features established for federal buildings/sites of their chosen security level each, using the referenced sources.

C. Practice

Day 2___Students remain in their five groups and are asked to consider the security standards recommended by the referenced Department of Justice Study "Vulnerability Assessment of Federal Facilities". They should discuss the relation of these standards to building site and construction. Each group should decide on what they consider to be the most important recommendations for an airport.

D. Independent Practice

Day 3___Students are asked independently to select five of the security standards and to imagine (as if they were a terrorist) where and how they could try to attack or breach the security of an airport. They should share their thoughts with classmates to see how many their ideas relate.

E. Accommodations (Differentiated Instruction)

Some students may be most skillful researching the scientific basis and technical aspects of a respective security standard.

Some students may be most comfortable with diagramming the physical layout of the airport and its site, locating points of vulnerability.

Some students may have a natural affinity for illustrating the techniques in an airport building as called for in the federal security standards.

Some students might be most adept at organizing a team presentation and writing/editing the narrative of the team report to be made to the rest of the class.

F. Checking For Understanding

No matter what distinctive task a student embraces as a team member and as an individual she/he should be able to demonstrate a comprehensive understanding by the recount and summation of all that has been presented by all five teams. Each student contributes to the discussion to demonstrate knowledge of conducting a threat assessment, identifying vulnerabilities, and producing a risk assessment for an airport site and terminal.

G. Closure

Students should document their experience in final report form, annotating their rationale for the threat assessment, vulnerabilities assessment and risk analysis.

9 Evaluation

Students are to be evaluated on the clarity with which they present the content of their reports, including:

- Concise but thorough writing;
- Annotation of appropriately excerpted/constructed illustrations;
- Logic and organization of the presentation;
- Quality of the report formatting.

10 Teacher Reflection

To be completed by the teacher after teaching the lesson.

11 Resources & Media

Computer in classroom with internet connection; Audio and Video Output Devices for the Computer; In-class Worksheets and Handouts

Security Centers

Anti-Terrorism Force Protection (DOD) (Limited access)

Defense Threat Reduction Agency

Department of Defense (DOD) Anti-terrorism body—Pentagon's J34

Federal Emergency Management Agency (FEMA) All-Hazard Mitigation Program on Anti-terrorism

Naval Facilities Engineering Service Center (NFESC), Security Engineering Center of Expertise ESC66 - E-mail: securityeng@nfesc.navy.mil

USAF Electronic System Center (ESC), Hanscom AFB

U.S. Army Corps of Engineers, Electronic Security Center

U.S. Army Corps of Engineers, Protective Design Center

U.S. Department of Defense

U.S. Department of Homeland Security

Organizations and Associations

The American Institute of Architects (AIA) Security Resource Center

American Society of Civil Engineers (ASCE)

American Society of Industrial Security (ASIS)

Battelle Memorial Institute, National Security Program

Center for Strategic and International Studies (CSIS)

Centers for Disease Control and Prevention (CDC)

Federal Facilities Council (FFC) Standing Committee on Physical Security and Hazard Mitigation (Sponsored by National Academies of Science)

International CPTED Association (ICA)

National Academy of Sciences

National Defense Industrial Association (NDIA)

National Institute of Standards and Technology (NIST)

Postal Security Action Group (PSAG)

Protective Glazing Council (PGC)

Security Industry Association (SIA)

Society of American Military Engineers (SAME)

The Infrastructure Security Partnership (TISP)

U.S. Army Soldier and Biological Chemical Command (SBCCOM)

Trade Journals/Magazines

Architectural Design for Security and Security and Technology Design by Donald M. Rochon. June 1998.

Designing for Crime and Terrorism, Security and Technology Design by Randall I. Atlas. June 1998.

Government Security

Security Magazine

Security Solutions Online: Access Control and Security Systems

Security through Environmental Design, Security and Technology Design by Robert Pearson. September 1997.

Training Courses

FEMA E155—Building Design for Homeland Security

Others

Agent-Based Simulation of Human Movements During Emergency Evacuations of Facilities. (PDF 168 KB, 10 pgs) Joseph L. Smith, PSP, Applied Research Associates, Inc.

Anthrax-Contaminated Facilities: Preparations and a Standard for Remediation by the Congressional Research Service. 2005.

Creating Defensible Space by Oscar Newman. Washington, DC: U.S. Department of Housing and Urban Development, April 1996.

National Symposium of Comprehensive Force Protection, Society of American Military Engineers (SAME), Charleston, SC, Oct 2001. Lindbergh & Associates.

NIST WTC Investigation: Building Standards and Codes: Who is in Charge?

Protecting Building Occupants from Biological Threats—Website from the Center for Biosecurity of UPMC that includes useful information about biological threats to building occupants, practical steps for reducing risk, and costs and benefits of risk reduction measures, along with a wealth of related materials and additional resources

ATTACHMENT # 1

The United States and the rest of the world face a dynamic and uncertain security environment from the forces of international terror.

The combination of the greater use of international travel, modern information access systems which propagate inexpensive and easy to manufacture explosive technology, and the increased number of financial supporters of terrorist activities gives many factions the ability to strike at nearly any "soft" target desired.

Explosive devices can be packaged or hidden in nearly any configuration imaginable. People and facilities are vulnerable to bombing attacks from terrorists. Incidents such as the African embassies, Khobar Towers and the Oklahoma City bombings dramatically underscore the need to take bombing threats seriously both on foreign soil and in the United States. Military facilities and personnel are prime targets for terrorist bombings, due to their high profile and symbolic value to the terrorists.

Searching for Evidence of Anthrax

FBI Photo

Terrorist Vehicle Bomb

FBI Photo

[2] Excerpted from the public domain Naval Facilities Engineering Command web site:

https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/atfp/atservices_tab

Tactical Bomb Components

FBI Photo

Attack on Khobar Towers

Photo by: Senior Airman Sean Worrell, USAF

Attack on U.S.S. Cole

DoD Photo